UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

ANGIE KIELISZEWSKI AND LYNNANN WARE, individually and on behalf of all others similarly situated, Plaintiffs, v. RELIAS LLC, Defendant.	Case No. 5:25-cv-00043-M-RN **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Angie Kieliszewski and LynnAnn Ware (together, "Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Relias LLC ("Defendant" or "Relias") for its violations of the Video Privacy Protection Act, 18 U.S.C. § 2710 ("VPPA"). Plaintiffs' claims arise from Defendant's practice of knowingly disclosing to a third party, Meta Platforms, Inc. ("Meta"), information which identifies the specific prerecorded audio visual material Plaintiffs and similarly situated consumers have requested or obtained from Defendant's websites, https://nurse.com/ and https://www.freecme.com/[1] (together the "Websites"). Plaintiffs make the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to

[1] Plaintiffs' claims include not only the root websites https://nurse.com and https://www.freecme.com, but also any page included within those Websites (e.g., https://www.freecme.com/courses).

allegations pertaining specifically to themselves or their counsel, which are based on personal knowledge.

I. NATURE OF THE CASE

1. Plaintiffs bring this consumer privacy class action to protect the privacy rights granted to them under federal law – rights Relias violates by knowingly disclosing its consumers' personally identifiable information to Meta. Specifically, Defendant knowingly discloses information which includes its consumers' identities alongside the titles of the prerecorded audio visual materials they request or obtain from the Websites.

2. Defendant's Websites offer a large volume of prerecorded audio-visual materials which provide education and knowledge about various topics related to healthcare, and through the Websites, Defendant's customers can request or obtain such material.

3. The VPPA prohibits "video tape service providers," such as Defendant, from "knowingly disclos[ing]" consumers' personally identifiable information ("PII"), defined as "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710 et seq.

4. Defendant systematically transmits its consumers' PII to Meta using a snippet of programming code called the "Meta Pixel," which Defendant chose to

install and configure on its Websites. The Websites operate and use the Meta Pixel in the same or a substantially similar way.

5. The PII Defendant knowingly discloses to Meta in a single transmission via the Meta Pixel includes the consumer's Facebook ID ("FID") in conjunction with the title and URL of the specific prerecorded video materials that the consumer requests or obtains on its Websites.

6. An FID is a unique sequence of numbers linked to a specific Facebook profile. A Facebook profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person including his or her name, photographs, and educational history). Entering "Facebook.com/[FID]" into a web browser returns the Facebook profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name, but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta information that reveals a particular person requested or obtained prerecorded video content (the PII at issue) on Defendant's Websites.

7. Defendant did not install the Pixel by accident, nor without an understanding as to its purpose or its function. When Defendant obtained the base code to install the Pixel, it agreed to Meta's Business Tools Terms which clearly

describe the Pixel's operation. Defendant installed the Pixel to obtain its benefits – enhanced marketing outcomes leading to increased visitors and higher revenue.

8. Defendant may also disclose Plaintiffs' PII via Meta's Conversions API ("CAPI"), a server-side technology that shares users' website interactions and personal information with Meta directly from the website host's server.

9. Defendant discloses its consumers' PII to Meta without obtaining their consent, which is prohibited under the VPPA.

10. Accordingly, on behalf of themselves and the putative Class members defined below, Plaintiffs bring this First Amended Class Action Complaint against Defendant for knowingly disclosing their and the Putative Class members' PII to Meta, in violation of the VPPA.[2]

II. PARTIES

A. Plaintiff Angie Kieliszewski

11. Plaintiff Angie Kieliszewski ("Plaintiff Kieliszewski") is, and at all times relevant hereto was, a citizen and resident of Montgomery County, Pennsylvania.

12. Plaintiff Kieliszewski became a consumer of Defendant's Website, nurse.com, on or about April 12, 2024. Plaintiff Kieliszewski has also been a Meta user with a unique Facebook profile page, and FID, during the entire class period.

[2] This First Amended Class Action Complaint is filed within twenty-one (21) days of service. Fed. R. Civ. P. (15)(a)(1)(A).

13. When she created her account with Defendant, Defendant required Plaintiff Kieliszeski to provide her name, email address, professional specialties, degree, phone number and zip code. In exchange for providing her personal information, Plaintiff Kieliszewski was granted access to prerecorded audio visual materials unavailable to the general public.

14. Defendant used the information Plaintiff Kieliszeski submitted when establishing her account to contact her during the class period, such as by sending her promotional emails to her email address.

15. During the relevant period, Plaintiff Kieliszeski's Facebook profile included publicly available information specifically and uniquely identifying her, including but not limited to her full name, education, and photographs of herself and her family. Any person could use Plaintiff Kieliszeski's unique FID to link directly to her Facebook page and view this publicly available, uniquely identifying information.

16. During the relevant period, Plaintiff Kieliszewski requested or obtained courses containing prerecorded audio visual material from Defendant using her Internet-connected device and web-browsing software installed on that device. Plaintiff Kieliszeski requested or obtained prerecorded audio visual material, including stand-alone courses and the Unlimited CE subscription.

17. When Plaintiff Kieliszewski requested or obtained Defendant's prerecorded audio visual material using her browser, she was logged into her Facebook account from the same browser.

18. Just as depicted in *Figures* 3-6 below, Defendant disclosed to Meta the titles of the prerecorded audio visual materials Plaintiff Kieliszewski requested or obtained along with the c_user cookie containing her FID, which is directly linked to Plaintiff Kieliszewski's personal Facebook profile, in the same network transmission.

19. Plaintiff Kieliszewski never consented, agreed, authorized, or otherwise permitted Defendant to disclose her PII to Meta in a manner consistent with the VPPA's requirements.

20. Because Defendant disclosed Plaintiff Kieliszewski's PII to Meta during the applicable statutory period, Defendant violated Plaintiff Kieliszewski's rights under the VPPA and invaded her statutorily conferred right to keep such information (which bears on her personal affairs and concerns) private.

B. Plaintiff LynnAnn Ware

21. Plaintiff LynnAnn Ware ("Plaintiff Ware") is, and at all times relevant hereto was, a citizen and resident of Chester County, Pennsylvania.

22. Plaintiff Ware became a consumer of Defendant's Website, nurse.com, on or about December 2018. Plaintiff Ware has also been a Meta user with a unique Facebook profile page, and FID, during the entire class period.

23. When she created her account with Defendant, Defendant required Plaintiff Ware to provide her name, email address, professional specialties, degree, phone number and zip code. In exchange for providing her personal information, Plaintiff Ware was granted access to prerecorded audio visual materials unavailable to the general public.

24. Defendant used the information Plaintiff Ware submitted when establishing her account to contact her during the class period, such as through sending her promotional emails to her email address.

25. During the relevant period, Plaintiff Ware's Facebook profile included publicly-available information specifically and uniquely identifying her, including but not limited to her full name, education, and photographs of herself and her family. Any person could use Plaintiff Ware's unique FID to link directly to her Facebook page and view this publicly available, uniquely identifying information.

26. During the relevant period, Plaintiff Ware requested or obtained courses containing prerecorded audio visual material from Defendant using her Internet-connected device and web-browsing software installed on that device. Plaintiff Ware requested or obtained prerecorded audio visual material, including the course "Heroin: The Opioid Crisis."

27. When Plaintiff Ware requested or obtained Defendant's prerecorded audio visual material using her browser, she was logged into her Facebook account from the same browser.

28. Just as depicted in the Allen Carney exemplars in *Figures* 3-6 below, Defendant disclosed to Meta the titles of the prerecorded audio visual materials Plaintiff Ware requested or obtained along with the c_user cookie containing her FID, which is directly linked to Plaintiff Ware's personal Facebook profile, in the same network transmission.

29. Plaintiff Ware never consented, agreed, authorized, or otherwise permitted Defendant to disclose her PII to Meta in a manner consistent with the requirements under the VPPA.

30. Because Defendant disclosed Plaintiff Ware's PII (including her FID and the titles of the audio visual material she requested or obtained from Defendant) to Meta during the applicable statutory period, Defendant violated Plaintiff Ware's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

C. Defendant Relias LLC

31. Defendant is a foreign limited liability company organized under the laws of the State of Delaware with its headquarters and principal place of business at 1010 Sync St. Morrisville, NC 27560. Defendant is a leading online educational provider of educational material, including prerecorded audio visual materials on various topics such as accredited skin & wound care, nursing, physical therapy, social work, diabetic wound care, ostomy management, and more.

32. Defendant owns and operates the Websites through which it knowingly

discloses its consumers' PII to third parties, including Meta. Defendant is "engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," and accordingly falls within the VPPA's definition of "video tape service provider." 18 U.S.C. § 2710(a)(4).

33. To request or obtain prerecorded videos on Defendant's Websites, a person must first create an account by providing their full name, email, phone number, specialty and degree.

34. After establishing their accounts, consumers may purchase audio visual materials in three ways, including:

a. Individual courses,

b. Standard and premium memberships (which grant consumers access to those same courses for free or at a discounted rate), and/or

c. State renewal packages (which contain courses tailored to each state's continuing education requirements).

35. Consumers are also given access to a number of free audio visual courses on the Websites.

36. Each time a consumer purchases an individual course or otherwise requests or obtains a course through their account, the Websites disclose their PII – FID and title of the audio visual material – to Meta via the Meta Pixel.

37. Defendant's Website, nurse.com, carries over one thousand online continuing education courses featuring prerecorded audio visual materials on

dozens of topics relevant to every nursing discipline and the nursing profession in general. Nurse.com also has a "Free Course" category which contains numerous courses linked directly to its sister website freeCME.com.

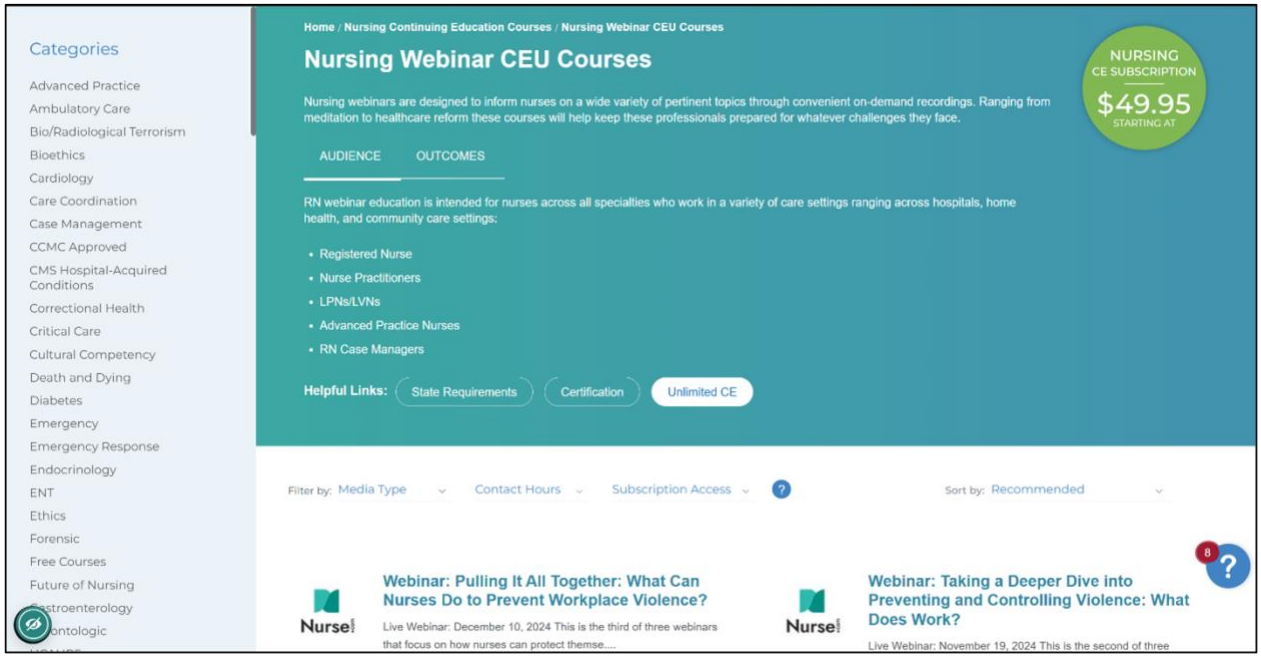

Figure 1

38. Defendant's Website, freeCME.com, carries a rotating catalogue of over 300 continuing education courses and webinars featuring prerecorded audio visual materials on specialties like Emergency Medicine, Psychiatry, Allergy & Immunology, and more.

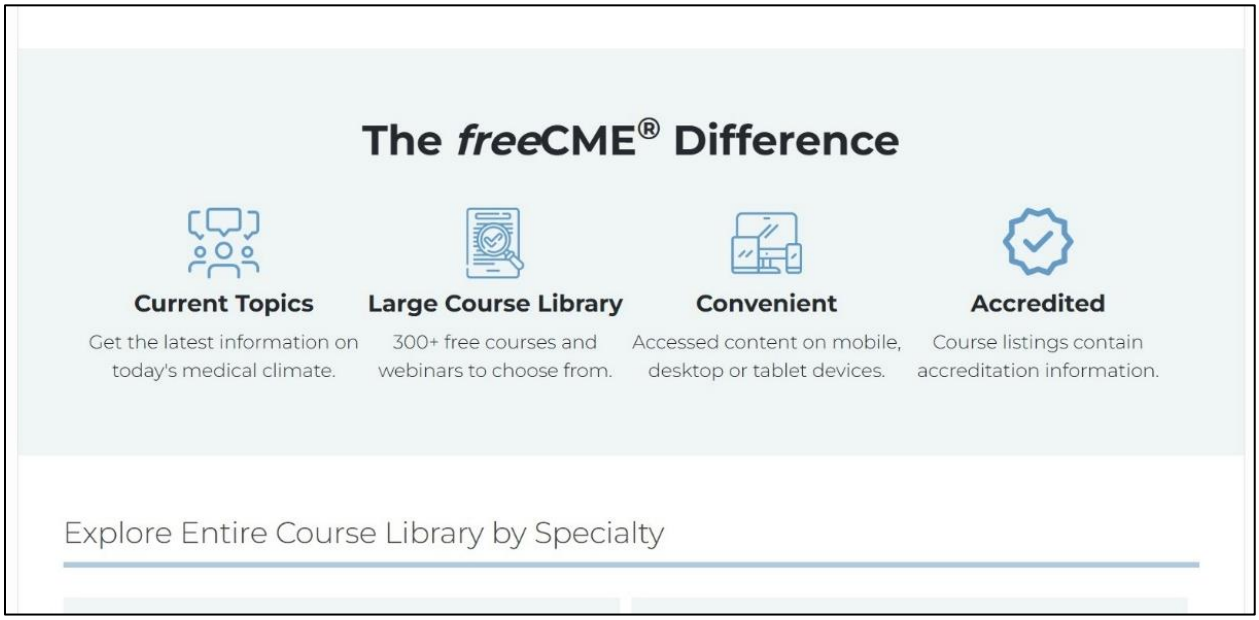

Figure 2

39. Defendant uses subject matter experts, including practitioners and industry leaders to produce courses tailored to meet nurse licensing requirements for all 50 states as well as Guam, Puerto Rico, the U.S. Virgin Islands, and Washington D.C.

III. JURISDICTION AND VENUE

40. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

41. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in Morrisville, North Carolina within this judicial District.

IV. BACKGROUND

A. The Video Privacy Protection Act

42. The VPPA is a robust privacy statute prohibiting companies (like Defendant) from knowingly disclosing to third parties (like Meta) PII about consumers (like Plaintiffs).

43. Specifically, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1).[3] The statute defines a "video tape service provider" as "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4). It defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

44. Leading up to the VPPA's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and

[3] The VPPA includes several exceptions, none of which are relevant here.

other audiovisual materials because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

45. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, the personal nature of such information, and the need to protect it from disclosure, is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id*.

46. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a more recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental

right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[4]

47. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[5]

48. In this case, however, Defendant deprived Plaintiffs and numerous other similarly situated persons of that right by systematically (and surreptitiously) disclosing their PII to Meta, without obtaining consent from them, as explained in detail below.

B. Personal Information Has Real Market Value

49. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything

[4] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury.

[5] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, franken.senate.gov (Jan. 31, 2012).

we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[6]

50. Over two decades later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a 26 billion dollar per year online advertising industry in the United States.[7]

51. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[8]

52. In fact, an entire industry exists where companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[9]

53. Data aggregation is especially troublesome when consumer information is disclosed to direct-mail advertisers. In addition to causing waste and

---

[6] Transcript, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[7] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), available at https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[8] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

[9] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), available at http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/ .

inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like Relias share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[10]

C. Consumers Place Monetary Value on Their Privacy

54. As the data aggregation industry has grown, so have consumer concerns regarding personal information.

55. A survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do protect their privacy online.[11] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[12]

56. Thus, as consumer privacy concerns grow, consumers increasingly incorporate privacy concerns and values into their purchasing decisions, and companies viewed as having weaker privacy protections are forced to offer greater

[10] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.
[11] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.
[12] *Id*.

value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[13]

57. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[14]

58. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[15] As such, where a business offers consumers a product or service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the consumer receives a product or service of less value than the product or service paid for.

---

[13] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), available at https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[14] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on Monetizing Privacy* (Feb. 27, 2012), available at https://www.enisa.europa.eu/publications/monetising-privacy.

[15] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

D. The Meta Pixel

59. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta."[16] Meta is now the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

60. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to monitor and track the actions taken by visitors to their websites and report them back to Meta. This allows companies like Defendant to build detailed profiles about their consumers and serve them with highly targeted advertising.

61. Additionally, the Pixel allows Meta to "match [] website visitors to their respective Facebook User accounts."[17] This is because Meta has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Facebook profile and thus identify the user by name[18] – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor. Each interaction sent to Meta via the Pixel (including by Defendant), is linked

[16] *See* Facebook, "Company Info," available at https://about.fb.com/company-info./.
[17] Meta, "Get Started – Meta Pixel," available at https://developers.facebook.com/docs/meta-pixel/get-started/.
[18] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

to and cross-referenced with all of the personal information Meta possesses about the user.

62. The Meta Pixel (including Defendant's Pixel) operates as follows: First, a user, through his or her browser, visits a website on which a Pixel is operational and requests information. In response to the user's request, the website instructs the user's browser what to display on the screen (i.e., content, products for sale, boxes with buttons that can be clicked, shopping carts, etc.). In addition to instructing the browser to load such content, the website instructs the browser to load the Pixel.

63. Like the webpage, the Pixel's code includes instructions for the user's browser, and it directs the browser to contact Meta with a report of what actions the user is taking on the webpage. These instructions inform the browser that certain actions taken by a user, such as viewing a page or clicking a button, should be shared with Meta in the form of a URL (see Figures 3a and 3b, below). Simultaneously, the Pixel instructs the browser to send to Meta an identifier that accompanies the URL—the FID, which is stored in the c_user cookie. Because the browser encounters the Pixel and downloads its instructions, it necessarily transmits this information to Meta.

64. As Meta's developer's guide explains, installing the Meta Pixel on a website allows Meta to track actions that users with Meta accounts take on the site.

Meta states that "Examples of [these] actions include adding an item to their shopping cart or making a purchase."[19]

65. Integral to this process, as detailed below, is that the website owner affirmatively installs a Pixel within its code for the exact purpose of creating these URLs and sharing them with Meta, because this process is how Meta can learn whether specific users are shown an advertisement and follow the advertisement through to view and/or purchase a product.

66. But for the website host's installation of the Pixel, a user's browser would not have reason to share the user's online browsing behavior or PII with Meta. None of the information transmitted to Meta via the Pixel is hashed or encrypted, including the FID, the URL, or the "event" information.

V. DEFENDANT'S PIXEL

A. Defendant Uses the Meta Pixel to Disclose its Consumers' PII

67. The manner in which Defendant configured its Pixel to transmit this information to Meta constitutes a disclosure of the personally identifiable information of its subscribers because each video requested or obtained (an "event") by each unique subscriber (through an "identifier") is disclosed to Meta.

68. An FID is a unique and persistent identifier that Meta assigns to each of its users. With nothing but a user's FID in hand, Meta can view that user's unique

[19] Meta, "About Meta Pixel," available at https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

Facebook profile. In fact, any person in possession of nothing more than a user's FID can locate the user's unique Facebook profile with the execution of one simple command within an internet browser (i.e., entering www.facebook.com/[FID] within the browser). An FID is nothing short of a link to the user's Facebook profile.

69. These two pieces of information are transmitted to Meta, via the Pixel, for every interaction it tracks. Thus, on every occasion on which the Pixel transmits information to Meta, an identifier is connected to and/or linked with the event in question—including when the event demonstrates that the user requested or obtained audio visual materials. When the transmission includes such information, it discloses the user's PII to Meta in violation of the VPPA.

70. Upon receipt of that transmission containing the URL, the name of the video content a subscriber requested or obtained, and the FID—all of which Defendant knowingly discloses to Meta—Meta learns the identity of the subscriber and the specific prerecorded audio visual material he requests or obtains from the Websites.

71. Through the Pixels it installed on the Websites, Defendant knowingly disclosed to Meta both the title of the prerecorded audio visual material a subscriber requested or obtained and the subscriber's FID in one single network transmission. Meta needs no additional information to connect a subscriber to the prerecorded audio visual material they requested or obtained on Defendant's Website. This transmission is depicted in the below example:

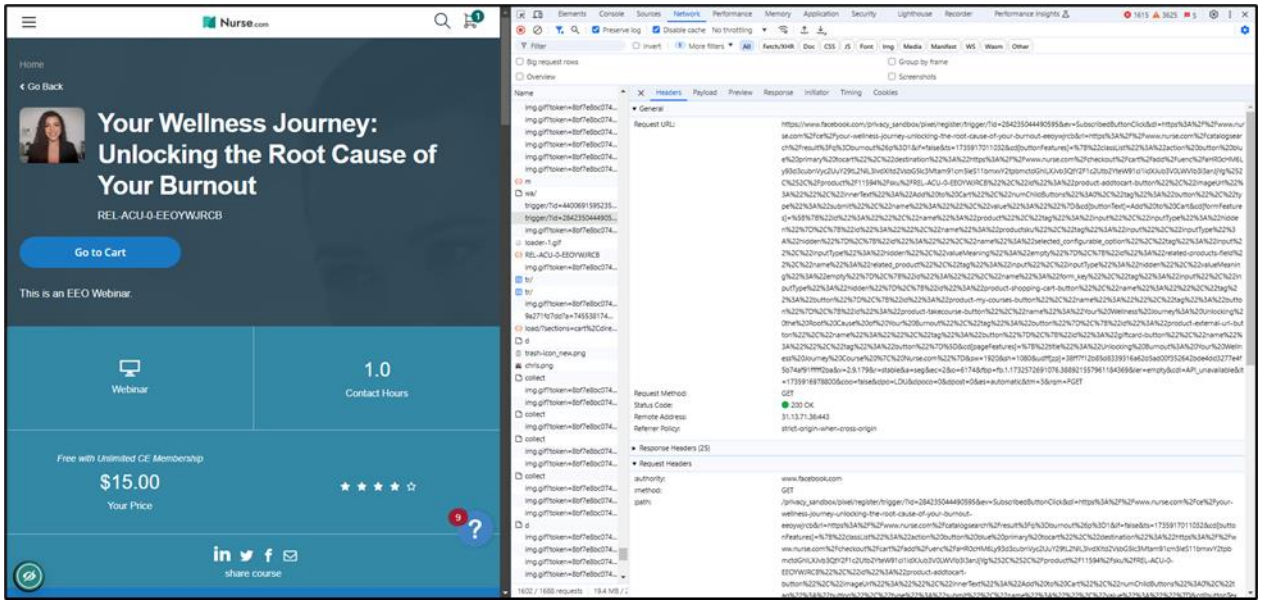

Figure 3-a

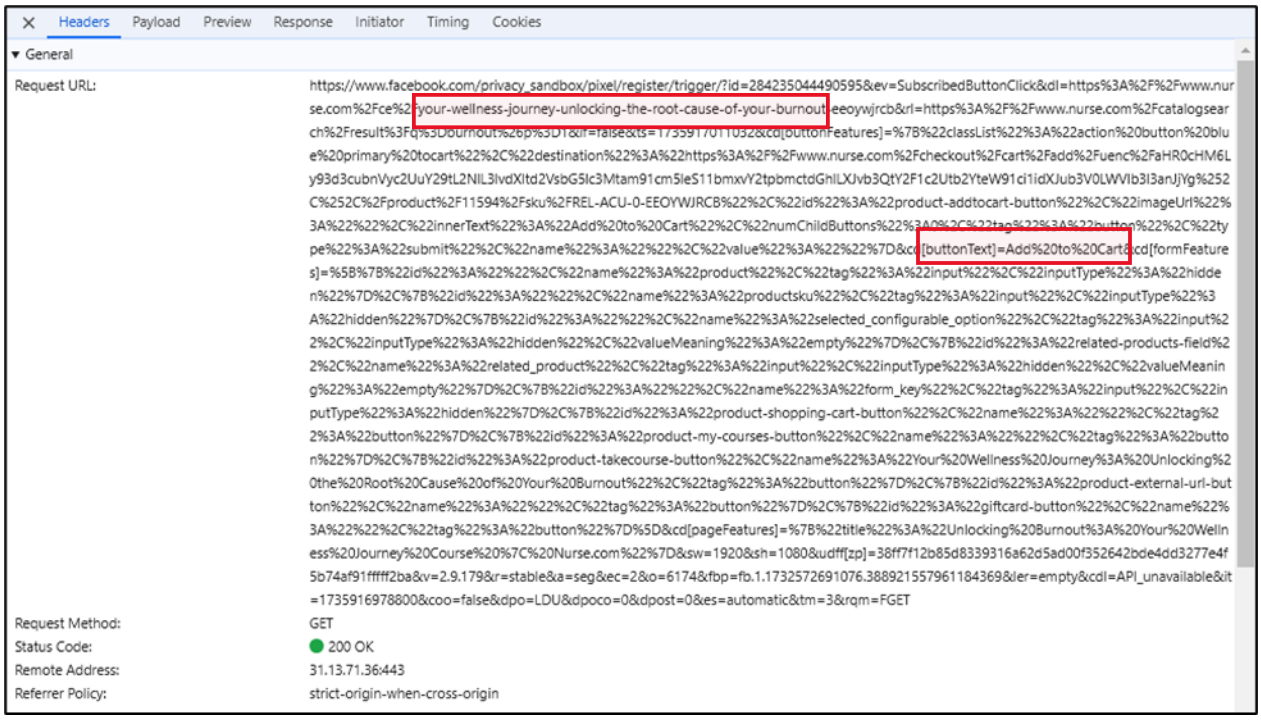

Figure 3-b

72. In this example, Defendant knowingly disclosed to Meta that Allen Carney[20] requested or obtained Defendant's prerecorded audio visual material "Your Wellness Journey: Unlocking the Root Cause of Your Burnout."

73. The FID is displayed as a numeric value referred to as the "c_user." The FID associated with Allen Carney's Facebook profile is "61567865736804."

74. The disclosure of the FID is coupled with the title of the prerecorded audio visual material the consumer requested, obtained or purchased within the URL transmitted to Meta:

[20] For the purposes of demonstrating how the Pixel transmits video titles alongside the user's FID in the c_user cookie, the screenshots in Figures 3-6 show the network traffic from watching videos on nurse.com from the same browser used to log into the Facebook account for Allen Carney.

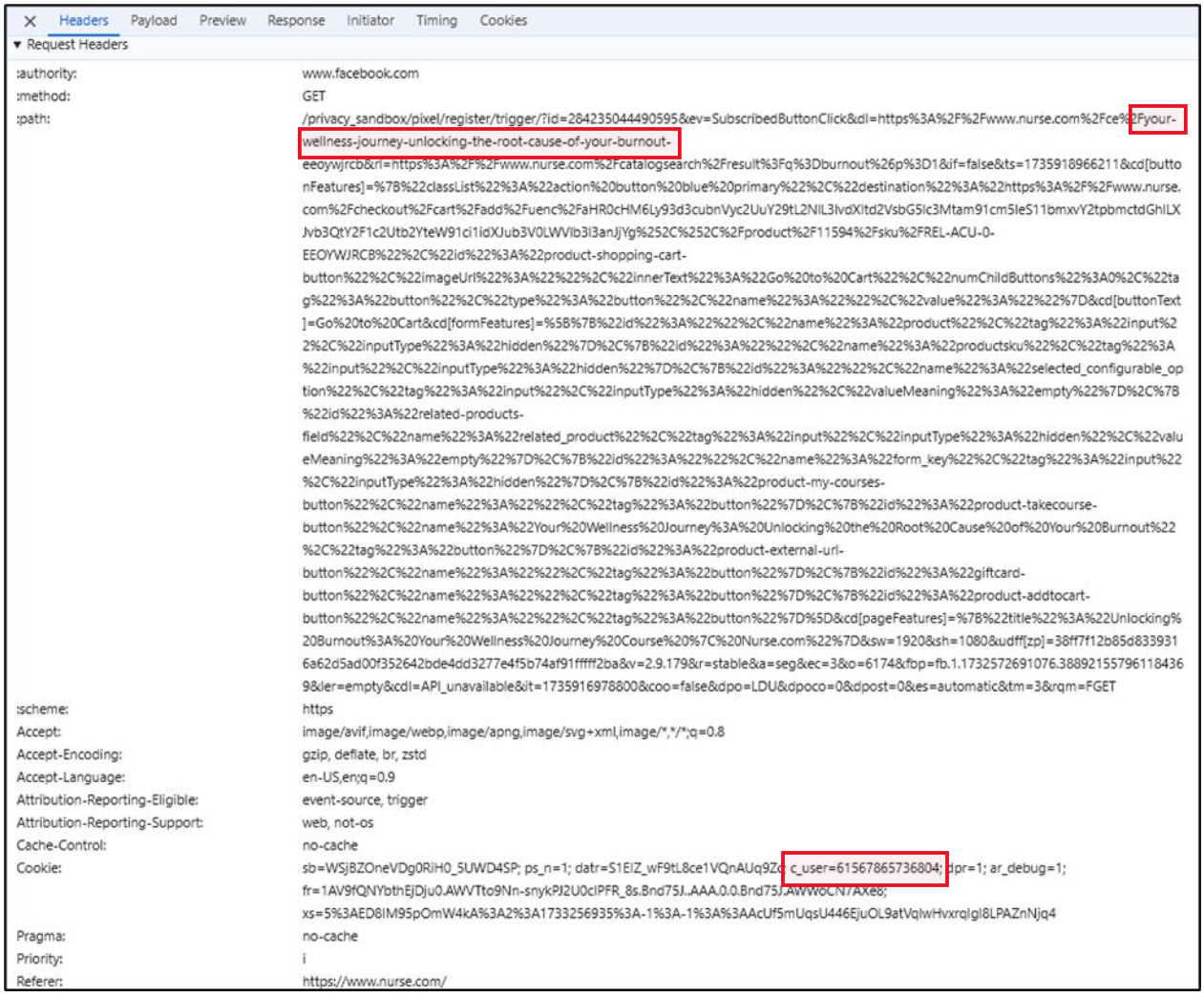

Figure 3-c

75. Through this transmission, Meta uniquely identifies the consumer requesting, obtaining, or purchasing the prerecorded audio visual material "Your Wellness Journey: Unlocking the Root Cause of Your Burnout." This individual is identifiable to any ordinary person in possession of this information because submitting "Facebook.com/61567865736804" into a browser's search bar (and nothing more), as illustrated by Figure 4, will direct the browser to populate Allen Carney's Facebook profile page, as can be seen in Figure 5.

Figure 4

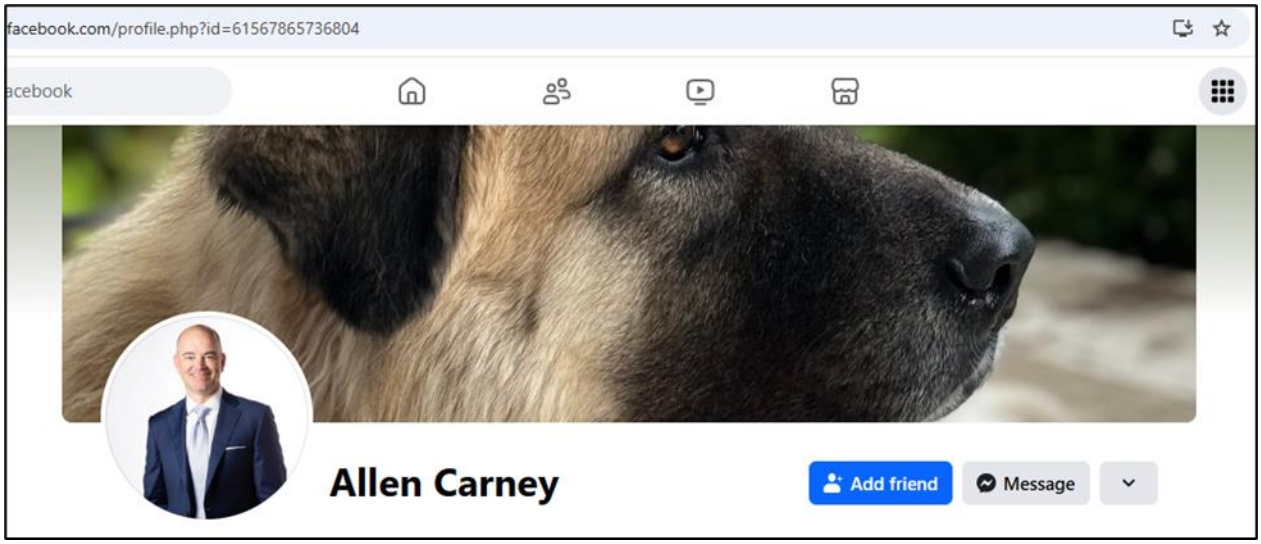

Figure 5

76. Just as depicted above for Allen Carney, this process occurs in exactly the same way for any Facebook user visiting the Website. Every time those users watch a video, Defendant transmits the title of the audio visual material they requested, obtained or purchased in conjunction with their FID.

77. The Pixels on each of the Websites function the same way. Just as shown in *Figure 3* (for nurse.com), the Pixel programmed onto freeCME.com also transmits consumers' FIDs along with the titles of the audio visual materials they request or obtain.

78. The PII shared by Defendant is personal and unique to Plaintiffs and each Class member.

79. Defendant intentionally programmed its Websites (by following step-by-step instructions from Meta's website) to include a Meta Pixel that systematically transmits to Meta the FIDs of its consumers in conjunction with the title of the prerecorded audio visual material they requested or obtained in order to take advantage of the targeted advertising and other informational and analytical services offered by Meta.

80. The VPPA establishes a right to privacy in U.S. citizens' PII regardless of the medium through which prerecorded audio visual material is requested or obtained. It imposes responsibilities on video tape service providers, like Defendant, to limit disclosure of PII.

81. Meta used the Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

82. If a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are

then able to "track [] the people and type of actions they take,"[21] including, as relevant here, the specific prerecorded video title requested or obtained on Defendant's Websites.

83. As demonstrated in the above Figures 3-5, Defendant's Pixel operated exactly as it was designed – providing Meta with a link to Plaintiffs' and the class members' Facebook profiles identifying the audio visual materials requested, obtained or purchased from the Website.

84. By knowingly disclosing its subscribers' PII to Meta, Defendant violates their privacy rights protected by the Video Privacy Protection Act.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the PII of its Consumers to Meta

85. Defendant operates its Websites in the U.S., accessible from a computer browser. Defendant, and Defendant alone, is responsible for the creation, configuration, and maintenance of its website.

86. Defendant purposefully installed and programmed the Pixel within its Websites operations, thus making the knowing choice to share subscribers' PII with Meta.

[21] Meta, "Retargeting: How to Advertise to Existing Customers with Ads on Facebook," available at https://www.facebook.com/business/goals/retargeting?checkpoint_src=any.

87. Meta's Business Tools Terms govern the use of Meta's Business Tools, including the Meta Pixel.[22] In order to obtain the base code[23] necessary to install the Pixel from Meta's online business portal, which provides substantial literature about the Pixel's purpose and function, Defendant was required to agree to Meta's Business Tools Terms.[24]

88. By using the Meta Pixel, Defendant agreed to send and knowingly did send "contact information," defined as "information that personally identifies individuals, such as names, email addresses, and phone numbers, that [Meta] uses for matching purposes," as well as "event data," defined as "information that you share about people and the actions that they take on your websites," instructing Meta to process that contact information and corresponding event data to match with User IDs on Meta products.[25]

89. Meta's literature about the Pixel is not cryptic: Meta clearly illustrates that the Pixel identifies specific online users, the specific actions they take on a website, and that Meta will use the information to target the specific user with specific advertising content:

---

[22] Meta, "Meta Business Tools Terms," available at https://www.facebook.com/legal/technology_terms. Meta for Developers, *Get Started*, Meta (2024) https://developers.facebook.com/docs/meta-pixel/get-started (last visited October 15, 2024).
[23] Meta, Business Tools Terms, https://www.facebook.com/legal/technology_terms (last accessed January 28, 2025).
[24] *Id*.
[25] *Id.*

> "The Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website…. Once you've set up the Meta Pixel, the pixel will log when someone takes an action on your website…. The pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. *You'll also have options to reach those customers again through future Meta ads*."[26] (emphasis added)

90. In its "Get Started" page, Meta explains "[b]y default, the Pixel will track URLs visited, domains visited, and the devices your visitors use."[27] In addition, website operators can also program their Pixel to track "conversions" (website visitor actions)[28] which are sent to the Facebook Ads Manager and the Facebook Events Manager to be used to analyze the effectiveness of ad campaigns and to define custom audiences to adjust and create new campaigns.[29]

91. Meta's "Get Started" page further explains how it can identify website visitors and match them to their Facebook pages: "[The Meta Pixel] relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can tally their actions in the Facebook

[26] Meta Business Help Center, *About Meta Pixel*, Meta https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited November 4, 2024).
[27] Meta for Developers, *Get Started*, Meta (2024) https://developers.facebook.com/docs/meta-pixel/get-started (last visited October 15, 2024).
[28] *Id*.
[29] Meta for Developers, *Conversion Tracking*, Meta (2024) https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited November 4, 2024).

Ads Manager so you can use the data to analyze your website's conversion flows and optimize your ad campaigns."

92. The purpose of the Meta Pixel – tracking and sending website visitor activity to Meta to match with the visitor's Facebook account – is thoroughly explained.

93. Defendant could easily have programmed its Websites so that none of its consumers' PII would be disclosed to Meta. A Pixel does not facilitate any necessary website operations whatsoever. But embedding the Pixel within a website's code enables a business, like Defendant, to benefit from the collection of measurable data that details how users interact with their websites, such as whether users initiate purchases on the website, what items they view, and, relevant here, the prerecorded audio visual material users request or obtain on a specific webpage.

94. In particular, Defendant's Pixel is configured to collect "Button Click" data, which betrays the possibility that Defendant is ignorant to this technology: Button Click tracking is not a default category tracked by the Pixel. Indeed, that Defendant's Pixel tracks this "event" is further evidence of its understanding of this technology because it must be affirmatively selected before the Pixel will record and transmit such events to Meta. "Button Click" data tracks which buttons or links subscribers click and when they do so.

Figure 6

95. The presence of settings on Defendant's Pixel beyond the default settings demonstrates that Defendant possesses a sophisticated understanding of this technology, its purpose, and how it works.

96. Meta's own literature illustrates that it developed advertising technology which sorts unique online users into custom audiences, and that its ability to create such audiences comes from data it obtains about specific, unique individuals visiting websites that host its data collection tools, such as Defendant.

97. While Defendant's Pixel was operational on its Website, Defendant knew that (i) the Pixel shared information which allowed Meta to uniquely identify the individuals interacting with Defendant's Website; (ii) the Pixel identified the specific interactions users took on its website—including the specific videos they requested or obtained; and (ii) that its Pixel collected and shared these items from subscribers to its website.

98. Defendant chose, programmed, and intended for Meta to receive the video content name and the subscriber's FID, and that the Meta Pixel disclosed its subscribers' personal viewing history to Meta.

99. Because its product is one of the best, Defendant had good reason to install Meta's advertising technology: in fact, as is *thoroughly* described by the materials Meta publishes about its advertising technology, Defendant not only *knew* the Pixel would share the above information with Meta – ***Defendant was counting on it.***

C. Conversions API

100. Upon information and belief, Defendant may have also configured a Meta product called Conversions API ("CAPI") to disclose consumers' PII to Meta as well.

101. CAPI operates directly from Defendant's server to transmit such information, unlike the Meta Pixel which operates from within Defendant's Websites' code and forces the user's browser to share information with Meta.

102. CAPI tracks users' interactions with the webpage, including their requests to view audio visual material, and personal information about them. It stores such information on the website owner's servers and transmits to Meta directly from its server, as opposed to the Pixel's operation, which shares such information by coopting the user's browser and forcing the browser to transmit identifying and interaction information to Meta.

103. Specifically, CAPI operates by sharing personal information stored on the website owner's server, such as Defendant's server, and transmits identifying information such as name, email address, or any other personal information the website owner configures it to transmit.

104. Indeed, Meta markets CAPI as "designed to create a direct connection between [Web hosts'] marketing data and [Meta]."[30] CAPI collects PII stored on the website host's server and sends such PII directly from Defendant to Meta.

105. Because CAPI is a server side technology, a user's attempts to thwart such privacy violations are rendered ineffective. Meta suggests website owners should use CAPI alongside the Pixel because it allows the host "to share website events [with Meta] that the pixel may lose.".[31] Thus, it is reasonable to infer that Meta's consumers who install the Meta Pixel—such as Defendant—will likewise implement the Conversions API consistent with Meta's advice.

CLASS ACTION ALLEGATIONS

106. Plaintiffs seek to represent a class defined as:

> All persons in the United States who (i) registered an account, (ii) requested, obtained or purchased prerecorded audio visual material from Defendant's Websites, and (iii) were logged into their Facebook profile during the period the Pixel was active on Defendant's Websites.

[30] Business Help Center, About Conversions API, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last accessed January 24, 2025).

[31] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Jan. 23, 2023).

107. The "Class Period" is from January 30, 2025 to the present.

108. Excluded from the Class is Defendant, any controlled person of Defendant, as well as the officers and directors of Defendant and the immediate family members of any such person. Also excluded is any judge who may preside over this cause of action and the immediate family members of any such person. Plaintiffs reserve the right to modify, change, or expand the Class definition based upon discovery and further investigation.

109. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

110. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to (a) whether Defendant knowingly disclosed Plaintiffs' and Class members' PII to Meta; (b) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; (c) whether Defendant should be enjoined from disclosing Plaintiffs' and Class members' PII; and (d) whether Plaintiffs and Class members are entitled to a statutory damage award of $2,500, as provided by the VPPA.

111. Plaintiffs' claims are typical of the claims of the members of the proposed Class because, among other things, Plaintiffs and members of the class sustained similar injuries from Defendant's uniform wrongful conduct, and their legal claims arise from the same events of wrongful conduct by Defendant.

112. Plaintiffs are adequate representatives of the Class because they are interested in the litigation; their interests do not conflict with those of the Class members they seek to represent; they have retained competent counsel experienced in prosecuting class actions; and they intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of all Class members.

113. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication of the common questions of law and fact, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment

of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

114. Plaintiffs also satisfy the requirements for maintaining a class under Rule 23(b)(2). Defendant acted on grounds that apply generally to the proposed Class, making final declaratory or injunctive relief appropriate with respect to the proposed Class as a whole.

115. Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(c)(4). Their claims consist of particular issues that are common to all Class members and are capable of class-wide resolution that will significantly advance the litigation.

CAUSE OF ACTION
Violation of the Video Privacy Protection Act
18 U.S.C. § 2710

116. Plaintiffs repeat the allegations asserted in the preceding paragraphs as if fully set forth herein.

117. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

118. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar

audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

119. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiffs and Class members are each a "consumer" within the meaning of the VPPA because they each requested or obtained prerecorded video content from Defendant's Websites.

120. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The PII that Defendant transmitted to Meta constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because it identified the titles of the prerecorded audio visual materials Plaintiffs and Class members requested or obtained from Defendant's Websites to Meta.

121. Defendant knowingly disclosed Plaintiffs' and Class members' PII to Meta via the Meta Pixel technology because Defendant intentionally installed and programmed the Meta Pixel code on its Websites, knowing that such code would transmit the specific title of the prerecorded videos requested, obtained or purchased in conjunction with consumers' unique identifiers (including FIDs).

122. Plaintiffs, like other putative class members, could be publicly identified through the use of their FID at the time they requested or obtained prerecorded video materials from Defendant's Website(s) because the FID is automatically linked to their Facebook account, which displayed their name, photograph, and other personally identifying information.

123. Defendant failed to obtain informed written consent from Plaintiffs or Class members authorizing it to disclose their PII to Meta or any other third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who requested or obtained prerecorded audio visual material its Websites (including Plaintiffs or Class members) informed, written consent that was given in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

124. By disclosing Plaintiffs' and Class members' PII, Defendant violated their statutorily protected right to privacy in their PII.

125. Consequently, Defendant is liable to Plaintiffs and Class members for damages in the statutorily set sum of $2,500. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek a judgment against Defendant Relias LLC as follows:

a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

b) For an order declaring that Defendant's conduct as described herein violated the VPPA;

c) For an order finding in favor of Plaintiffs and the Class and against Defendant on all counts asserted herein;

d) For an award of $2,500.00 to Plaintiffs and each Class member, as provided by 18 U.S.C. § 2710(c);

e) For an order permanently enjoining Defendant from disclosing the PII of its consumers to third parties in violation of the VPPA;

f) For prejudgment interest on all amounts awarded; and

g) For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiffs and the Class under Rule 23 and 18 U.S.C. § 2710(c).

Respectfully submitted,

Dated: February 24, 2025

By: */s/ Elliot O. Jackson*

HEDIN LLP

Elliot O. Jackson (*special appearance*)
Florida Bar No. 1034536
HEDIN LLP
1395 Brickell Ave., Suite 610
Miami, Florida 33131-3302
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
ejackson@hedinllp.com

Allen Carney (*special appearance* forthcoming)
acarney@cbplaw.com
Samuel Randolph Jackson (*special appearance* forthcoming)
sjackson@cbplaw.com
CARNEY BATES & PULLIAM, PLLC
One Allied Drive, Suite 1400
Little Rock, AR 72202
Telephone: (501) 312-8500
Facsimile: (501) 312-8505

Scott Harris (NC Bar 35328)*
sharris@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 West Morgan Street
Raleigh, NC 27603
Telephone: (919) 600-5003

Alton R. Williams*
Law Office of Alton R. Williams
4030 Wake Forest Road, Suite 300
Raleigh, NC 27609

Telephone: 919-340-0020
NC Bar. No. 38812
*Local Civil Rule 83.1(d) Attorneys
for Plaintiffs and Putative Class